

Les réserves de la CNIL sur le projet de loi renseignement | Le Net Expert Informatique



Les réserves de la
CNIL sur le projet de
loi renseignement

Il n'y aura pas de surveillance généralisée du citoyen, assure-t-on à Matignon, alors que le projet de loi renseignement doit être présenté jeudi en Conseil des ministres. Cela n'a pas empêché la Commission nationale de l'informatique et des libertés (CNIL) d'émettre un certain nombre de réserves sur ce texte, dont le calendrier a été accéléré après les attentats contre Charlie Hebdo et le supermarché casher de la porte de Vincennes.

Le projet de loi va permettre « une surveillance beaucoup plus large et intrusive », estime un pré-rapport dont « Les Echos » ont pu prendre connaissance. Si les objectifs du gouvernement paraissent « justifiés », « les atteintes portées au respect de la vie privée doivent être limitées au strict nécessaire », écrit la CNIL.

Trois dispositifs nouveaux (collecte automatique d'informations sur les réseaux, pose de sondes, sorte de mouchard permettant de collecter des informations en direct sur des personnes surveillées, et pose d'antennes à proximité de suspects) permettent de « collecter de manière indifférenciée un volume important de données » sur « des personnes relativement étrangères » aux suspects. « Ce changement a des conséquences particulièrement graves sur la protection de la vie privée et des données personnelles », avertit la CNIL.

« Aspiration massive de données »

Dans le détail, la détection « par un traitement automatique » des comportements suspects ressemble fort à de la surveillance généralisée. A Matignon, on se montre soucieux de faire de la « pédagogie » sur le sujet. L'objectif de la mesure, explique-t-on, est de détecter « les signaux faibles » permettant d'identifier des individus susceptibles de basculer dans le terrorisme. « Aujourd'hui, ceux qui partent n'ont pas été détectés avant leur départ [vers la Syrie, etc., ndr]. Or, 89 sont morts, dont un garçon de 14 ans », rappelle-t-on à Matignon.

Pour détecter ces inconnus, les agents veulent pouvoir analyser les flux de données, savoir qui communique avec qui, et quels sont les sites jihadistes visités. Pas d'autres moyens donc que de faire de la surveillance sur le réseau des opérateurs. « Nous voulons insérer dans les équipements des opérateurs des boîtes noires contenant des algorithmes identifiant des comportements marqueurs », précise Matignon. Si en théorie, la disposition pourrait s'appliquer aux géants du Net, les agents de l'Etat préfèrent d'abord aller traiter avec les opérateurs télécoms, considérant qu'ils sauront se montrer plus ouverts à leurs requêtes.

Inévitablement, une partie des flux échappera aux services, Google ayant depuis les révélations d'Edward Snowden chiffré l'ensemble des connexions de ses utilisateurs.

Quant à la captation en temps réel des données géolocalisées de personnes mises sous surveillance (3.000 personnes environ), elle est assimilée par la CNIL à un dispositif « d'aspiration massive et directe des données par l'intermédiaire de la pose de sondes ». Enfin, le système « IMSI Catcher » (pose d'antennes relais à proximité d'un suspect) permet aussi d'intercepter des informations sur des personnes n'ayant rien à voir avec les faits, regrette la CNIL.

De leur côté, les interceptions de sécurité – les fameuses écoutes – ne sont plus « exceptionnelles », note la CNIL, même si le texte « renforce les modalités de contrôle ». Surtout, la loi donne la possibilité « par réaction en chaîne » d'écouter « des personnes qui n'auraient pas été en relation avec la personne surveillée ».

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.lesechos.fr/tech-medias/hightech/0204235783787-les-reserves-de-la-cnil-sur-le-projet-de-loi-renseignement-1103298.php>

Par Sandrine Cassini

Projet de loi relatif au

renseignement | Le Net Expert Informatique

✕	Projet de loi relatif au renseignement
Le Conseil d'État a été saisi le 20 février 2015 et le 5 mars 2015 du projet de loi relatif au renseignement.	
<p>Ce projet de loi définit la mission des services spécialisés de renseignement et les conditions dans lesquelles ces services peuvent être autorisés, pour le recueil de renseignements relatifs à des intérêts publics limitativement énumérés, à recourir à des techniques portant sur l'accès administratif aux données de connexion, les interceptions de sécurité, la localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques, enfin à des mesures de surveillance internationale.</p> <p>Il instaure pour l'ensemble de ces techniques, à l'exception des mesures de surveillance internationale, un régime d'autorisation préalable du Premier ministre après avis et sous le contrôle d'une autorité administrative indépendante dénommée « Commission nationale de contrôle des techniques de renseignement », qui pourra recevoir des réclamations de toute personne y ayant un intérêt direct et personnel. Il fixe les durées de conservation des données collectées.</p> <p>Il prévoit un régime spécifique d'autorisation et de contrôle pour les mesures de surveillance et de contrôle des transmissions émises ou reçues à l'étranger.</p> <p>Il institue un recours juridictionnel devant le Conseil d'État ouvert à toute personne y ayant un intérêt direct et personnel, ainsi qu'à la Commission nationale de contrôle des techniques de renseignement, tout en prévoyant des règles procédurales dérogatoires destinées à préserver le secret de la défense nationale.</p> <p>Le Conseil d'État a veillé à ce que soient conciliées les nécessités propres aux objectifs poursuivis, notamment celui de la protection de la sécurité nationale, et le respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'est attaché à préciser et renforcer les garanties nécessaires à la mise en œuvre des techniques de renseignement, tenant en particulier à l'existence, d'une part, d'un contrôle administratif s'exerçant au moment de l'autorisation et en cours d'exécution, d'autre part, s'agissant d'une procédure administrative spéciale, d'un contrôle juridictionnel approfondi du Conseil d'État statuant au contentieux.</p>	
Lire la suite...	
<p>Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.</p> <p>Contactez-nous</p>	
<p>Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire...</p> <p>Source : http://www.legifrance.gouv.fr/Droit-francais/Les-avis-du-Conseil-d-Etat-rendus-sur-les-projets-de-loi/Projet-de-loi-relatif-au-renseignement-PRMX1504410L-19-03-2015</p>	

Après les attentats de Paris, simplification du blocage des sites Internet terroristes | Le Net Expert Informatique

Le Net Expert
INFORMATIQUE
Protection des données personnelles
Sécurité Informatique - Cybercriminalité



vous informe...

Après les #attentats de Paris, simplification du blocage des sites Internet terroristes

Le blocage administratif d'un site terroriste veut se passer d'autorité judiciaire? La Cnil y met bon ordre et place un juge au centre de la procédure en désignant Alexandre Linden en tant que personne qualifiée à s'assurer de la régularité d'un blocage.

Selon une information de nos confrères de L'Expansion, confirmée par la suite, la Cnil a nommé Alexandre Linden en tant que « personne qualifiée » pour encadrer le blocage administratif des sites incitant au terrorisme ou en faisant l'apologie. Cette nomination prendra effet dès sa publication au JO. La loi de novembre 2014 fait polémique, du fait notamment qu'une autorité administrative puisse exiger des FAI qu'ils interdisent l'accès à un site sans contrôle a priori d'un juge. Toutefois, cette procédure doit être encadrée par un membre de la Cnil.

L'article 6-1 de la LCEN (modifiée par la loi sur la lutte antiterroriste de novembre 2014) prévoit que la Commission nomme « en son sein » une personne en charge de « s'assurer de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste ». Pour cela, l'autorité administrative (l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication, ou OCLCTIC pour les intimes) doit lui transmettre « sans délai » les demandes de blocage, les listes d'adresses électroniques concernées et les raisons ayant motivé le blocage.

Un juge du blocage sans juge

Cette désignation est loin d'être anecdotique : Alexandre Linden (69 ans) est membre de la Cnil (depuis février 2014), mais aussi et surtout conseiller honoraire à la Cour de Cassation et ancien juge d'instruction. La Commission place donc un ancien magistrat au centre du dispositif de blocage par l'autorité administrative. Laquelle aura dès lors quelques difficultés à contourner le contrôle du juge, puisque celui-ci aura accès aux données relatives aux sites visés et pourra estimer la pertinence d'un blocage.

Toutefois, les recours seront limités, puisque les pouvoirs de cette « personne qualifiée » ne sont pas vraiment terrifiants : « si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin ». L'OCLCTIC doit déjà trembler d'effroi... Si jamais l'autorité devait ne pas suivre cet avis, « la personnalité qualifiée peut saisir la juridiction administrative compétente ». Soit faire appel au tribunal administratif et engager une longue procédure, au cours de laquelle le site restera bloqué. On restera donc prudent sur l'efficacité de cette fonction, malgré une nomination hautement symbolique.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

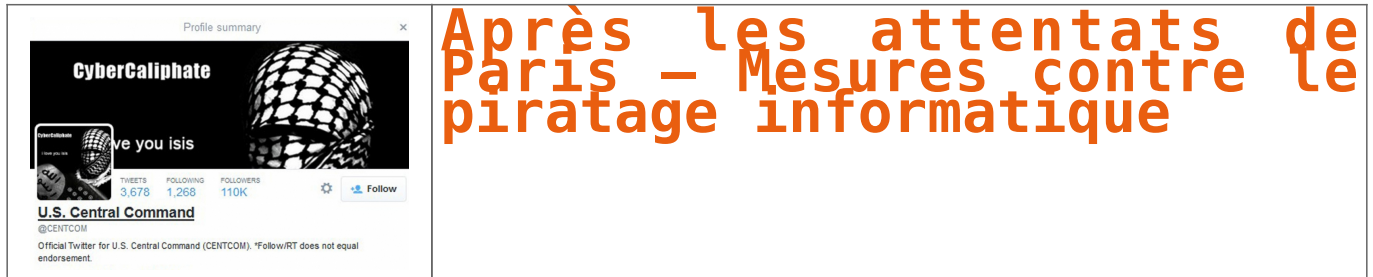
Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source

<http://www.linformaticien.com/actualites/id/35731/blocage-administratif-des-sites-la-cnil-nomme-un-juge.aspx> :

Après les attentats de Paris – Mesures contre le piratage informatique



The image shows a screenshot of a Twitter profile for U.S. Central Command (@CENTCOM). The profile picture is a globe with a grid pattern. The header text reads "CyberCaliphate" and "ve you isis". The profile statistics show 3,678 tweets, 1,268 following, and 110K followers. A "Follow" button is visible. A large orange text overlay is present on the right side of the screenshot, which reads "Après les attentats de Paris – Mesures contre le piratage informatique".

Profile summary x

CyberCaliphate

ve you isis

TWEETS 3,678 FOLLOWING 1,268 FOLLOWERS 110K

U.S. Central Command
@CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

Après les attentats de Paris – Mesures contre le piratage informatique

Un groupe se réclamant de l'Etat islamique (EI) a piraté, lundi, le compte Twitter du commandement de l'armée américaine au Moyen-Orient et en Asie centrale (US Central Command, CentCom).

Le #ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre les attaques informatiques.

Le ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre le piratage informatique quelques jours après les attentats jihadistes de Paris et à la suite d'une dizaine d'attaques dont ses sites internet ont été la cible. Deux de ces attaques « concernaient deux régiments de l'armée de Terre, dont une école », a ainsi déclaré à la presse le vice-amiral Arnaud Coustillière, responsable du pôle cyber-défense à l'état-major des Armées.

Au lendemain de la manifestation monstre, dimanche à Paris, en hommage aux 17 personnes tuées dans les attentats de la semaine dernière, « il a été décidé de monter le niveau de vigilance sur internet » et, « depuis mardi, je dispose d'une cellule de crise pour surveiller » les pirates informatiques, a ajouté le vice-amiral Coustillière. « Nous considérons que c'est une crise comme une autre, nous prenons des mesures de précaution et de vigilance (...) mais on ne peut pas parler de cyber-guerre », a-t-il ajouté, rappelant que le ministère de la Défense a environ 350 sites internet.

Profile summary

x



CyberCaliphate

I love you isis

TWEETS 3,678 FOLLOWING 1,268 FOLLOWERS 110K

U.S. Central Command

@CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

LE MINISTÈRE DE LA DÉFENSE VISÉ LE 6 JANVIER

« Les attaques contre le site de la Dicod (service de communication du ministère) continuent, il y a régulièrement des gens qui viennent tester le site de la Dicod », a précisé l'officier. « Pour moi, ces attaques sont la réponse à la manifestation de dimanche dernier, par des gens qui n'adhèrent pas à un certain nombre de valeurs », a-t-il dit.

Le site internet du ministère de la Défense avait déjà été cible le 6 janvier d'une attaque informatique revendiquée par le groupe Anonymous qui affirmait vouloir « venger » le militant écologiste Rémi Fraisse tué en octobre pendant la répression d'une manifestation.

Ces données sont à rapporter au fait que, selon les sources ouvertes et disponibles, mais qui n'émanent pas du ministère de la Défense, il y a eu depuis le 10 janvier de l'ordre de 20.000 attaques en France, par des « groupes plus ou moins structurés ou des hackers islamistes bien connus », contre les sites internet les plus variés, d'écoles, d'institutions, de pizzerias, etc., a ajouté le responsable. Ces attaques se font soit par saturation des sites, soit par pénétration ou « défacement », une opération qui consiste à remplacer la page d'accueil par une autre.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.parismatch.com/Vivre/High-Tech/Mesures-contre-le-piratage-informatique-691194>